FIG.1

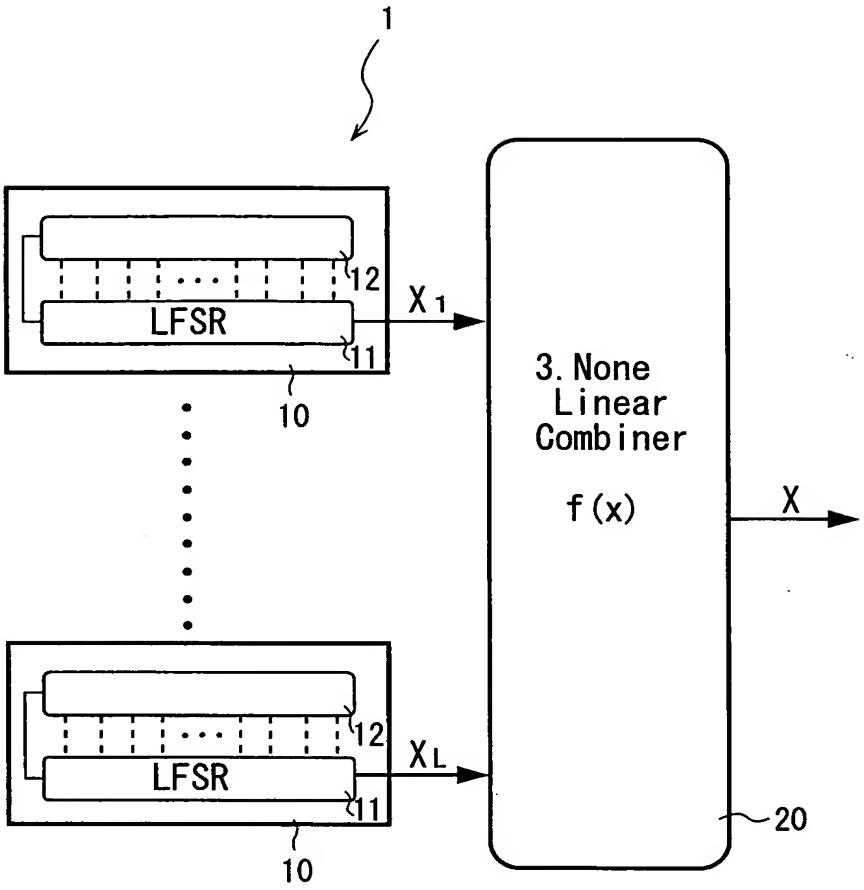


FIG.2

LSFR1	x^131+x^8+x^3+x^2+1
LSFR2	x^137+x^21+1
LSFR3	x^139+x^8+x^5+x^3+1
LSFR4	x^149+x^10+x^9+x^7+1
LSFR5	x^151+x^3+1
LSFR6	x^157+x^6+x^5+x^2+1
LSFR7	x^163+x^7+x^6+x^3+1
LSFR8	x^167+x^6+1

FIG. 3

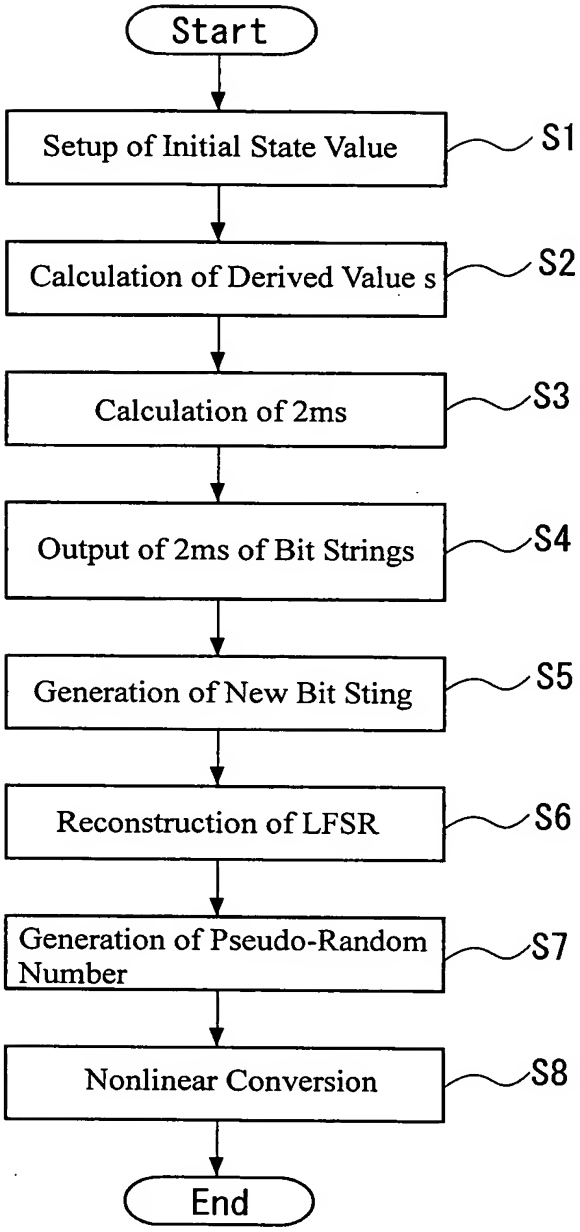

Start
Setup of Initial State Value
S1
Calculation of Derived Value s
S2
Calculation of 2ms
S3
Output of 2ms of Bit Strings
S4
Generation of New Bit Sting
S5
Reconstruction of LFSR
S6
Generation of Pseudo-Random Number
S7
Nonlinear Conversion
S8
End

FIG. 4

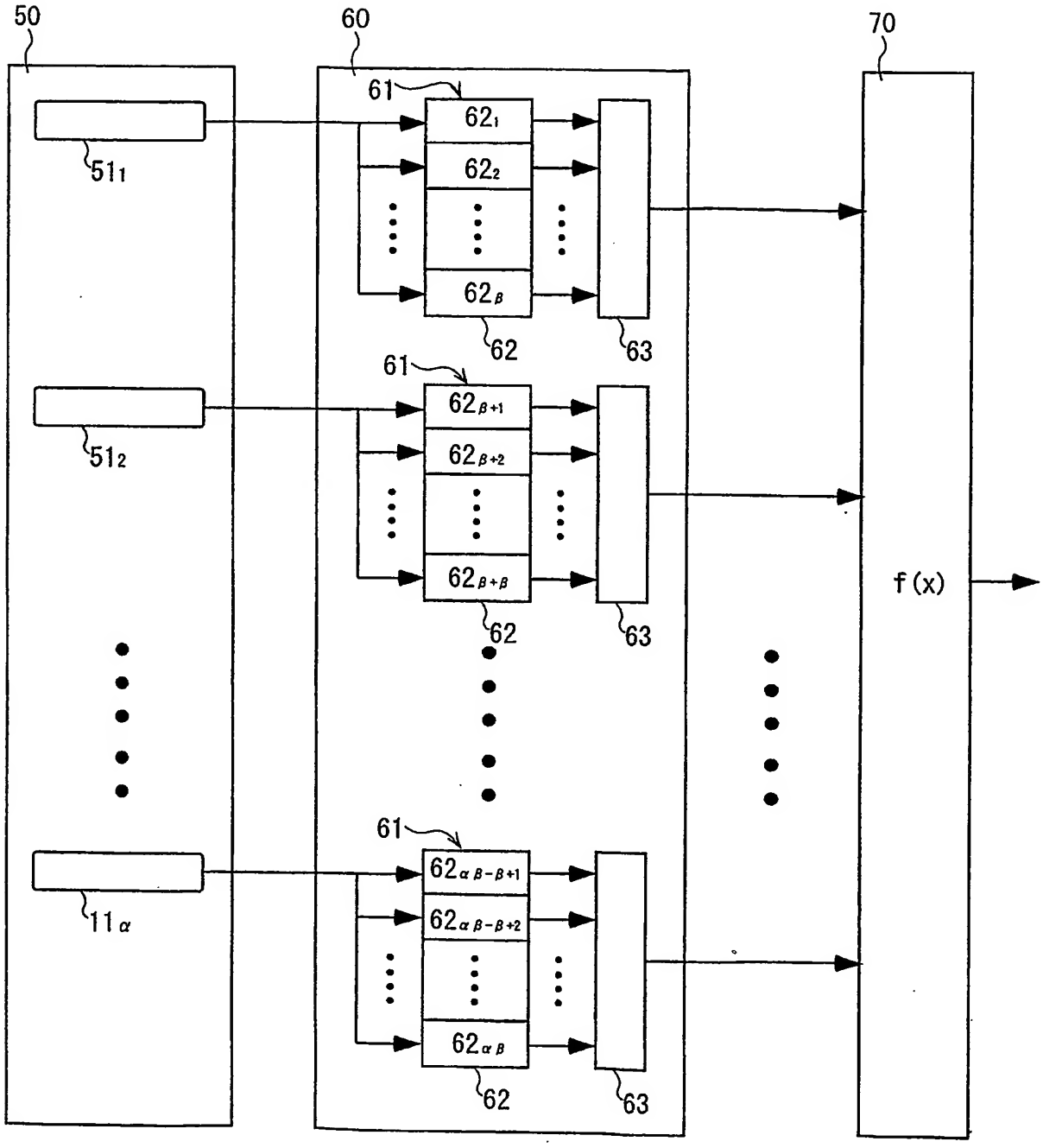

50
60
70
61
62_1
62_2
62_β
62
63
51_1
61
$62_{\beta+1}$
$62_{\beta+2}$
$62_{\beta+\beta}$
62
63
51_2
f(x)
61
$62_{\alpha\beta-\beta+1}$
$62_{\alpha\beta-\beta+2}$
$62_{\alpha\beta}$
62
63
11_α

FIG. 5

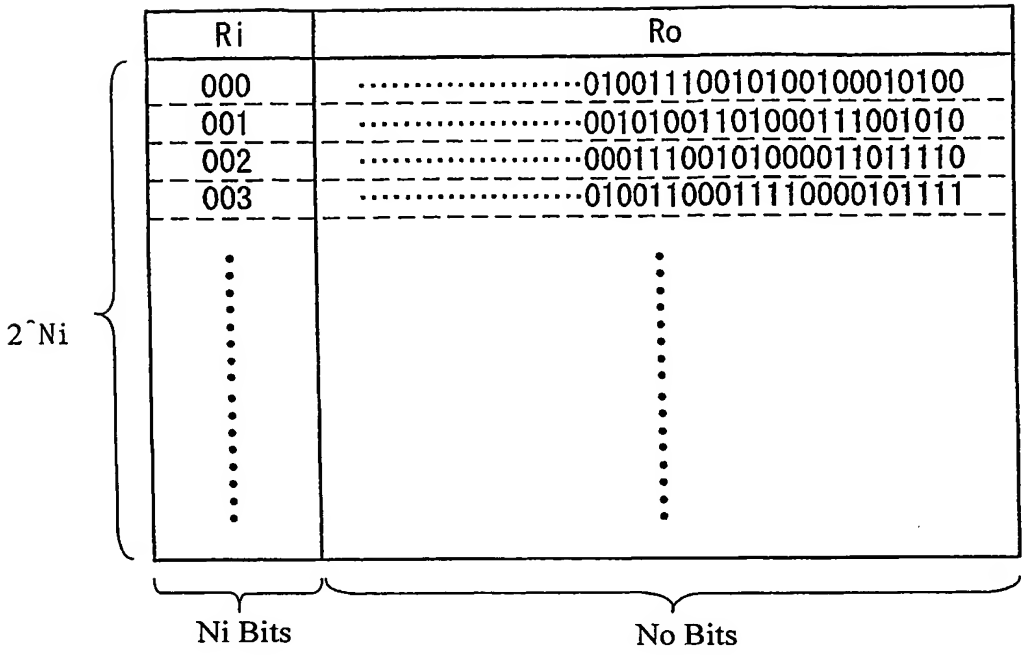


FIG. 6

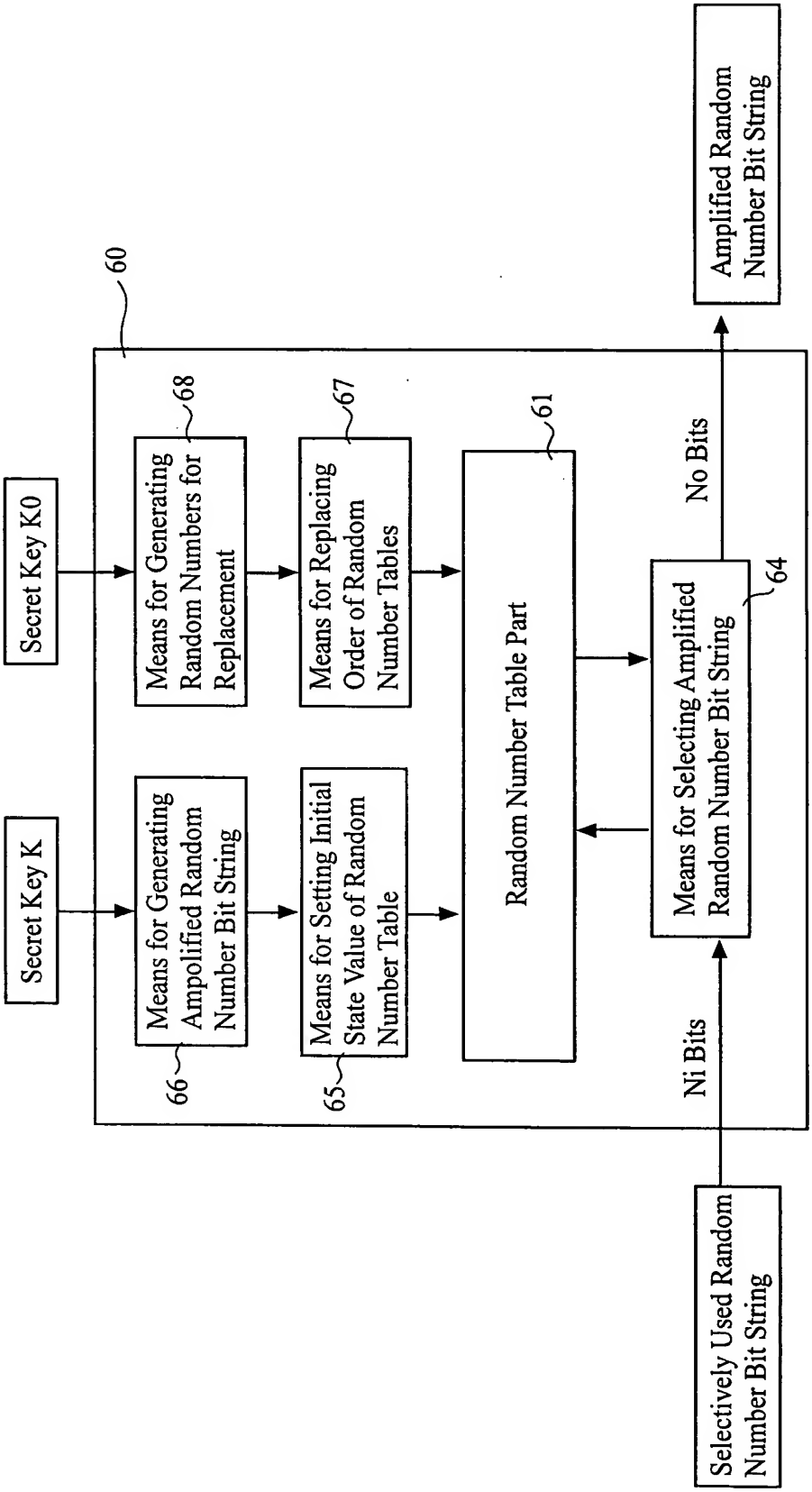

Secret Key K0
Secret Key K
Means for Generating Ampolified Random Number Bit String
Means for Generating Random Numbers for Replacement
Means for Setting Initial State Value of Random Number Table
Means for Replacing Order of Random Number Tables
Random Number Table Part
Means for Selecting Amplified Random Number Bit String
Amplified Random Number Bit String
Selectively Used Random Number Bit String
Ni Bits
No Bits
60
61
64
65
66
67
68

FIG.7

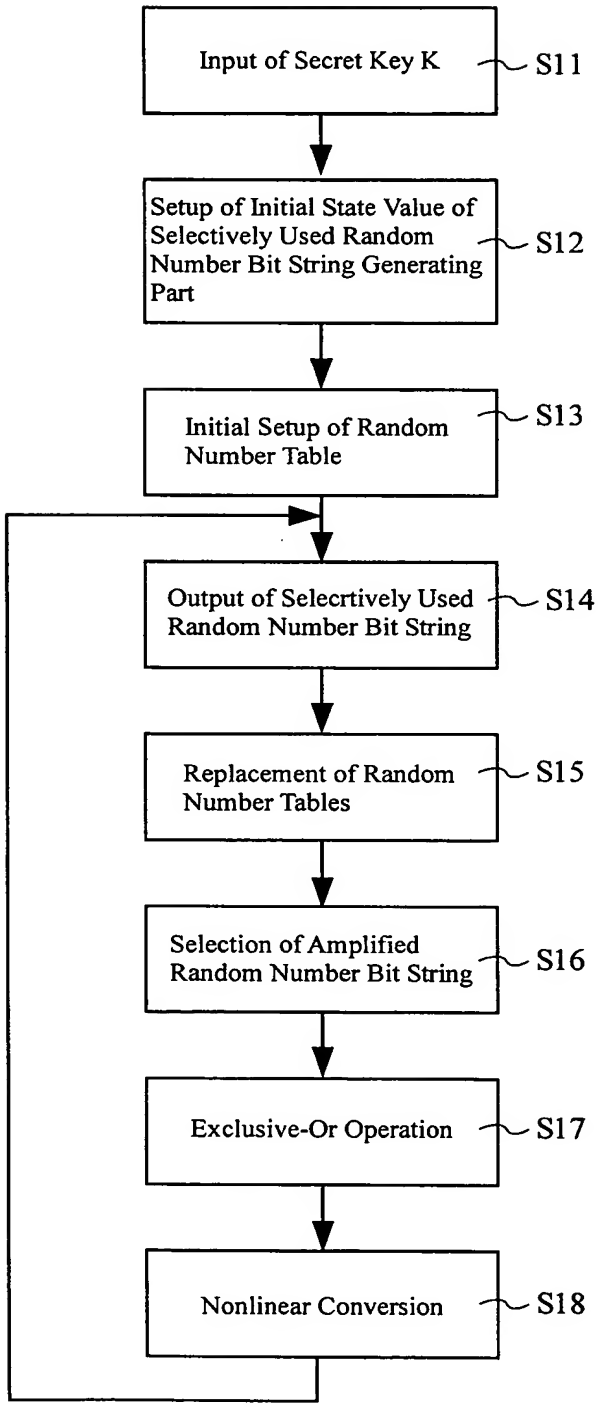

Input of Secret Key K
S11
Setup of Initial State Value of Selectively Used Random Number Bit String Generating Part
S12
Initial Setup of Random Number Table
S13
Output of Selecrtively Used Random Number Bit String
S14
Replacement of Random Number Tables
S15
Selection of Amplified Random Number Bit String
S16
Exclusive-Or Operation
S17
Nonlinear Conversion
S18

FIG. 8

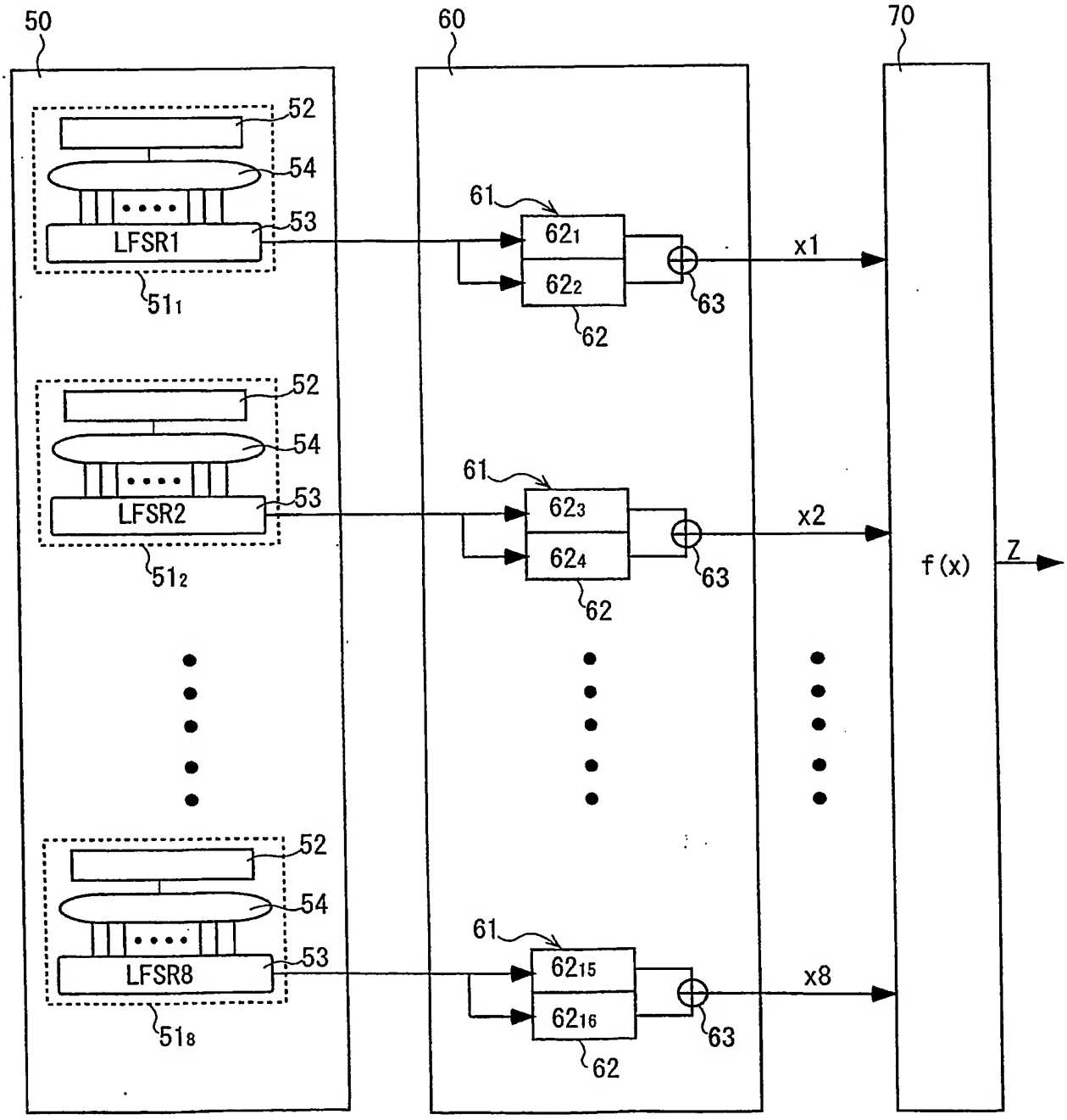

50
60
70
52
54
53
LFSR1
51₁
61
62₁
62₂
62
63
x1
LFSR2
51₂
62₃
62₄
x2
f(x)
Z
LFSR8
51₈
62₁₅
62₁₆
x8

Fig. 9

In case of $\alpha = 8$, $\beta = 2$, Ni=2^16, Lk=128

Selectively Used Random Number Bit String Corresponding to Output Means 61_1

Selectively Used Random Number Bit String Corresponding to Output Means 61_2

Selectively Used Random Number Bit String Corresponding to Output Means 61_n

Ri	Ro
0	0101101011000010110
1	1011010110001011 00
2	1010110101100010 11
3	0101101011011011 0
.	.
.	.
.	.
255	0101101000101010 10
0	0010101011000101 10
1	1010111010001011 00
2	0001011010110101 11
3	0110110101101011 01
.	.
.	.
.	.
255	0010101101011001 10
0	1010100100101010 10
1	1011010110001011 10
2	1110101001100010 11
3	0101101101010110 11
.	.
.	.
.	.
255	1101011010000101 10
0	1000101100101101 01
1	0010111000101101 01
2	0101101011001010 11
3	0011010110101101 11
.	
.	
.	
255	1101001011010100 10
	↓
0	0100110110101100 01
1	0101101101011001 00
2	1100010110101101 10
3	0110111001110101 10
.	.
.	.
.	.
255	0101011011000110 01
0	1101101101110010 10
1	1001101101110111 00
2	0110101011100110 10
3	0110110101110110 01
.	.
.	.
.	.
255	0101010101100011 01

FIG.10

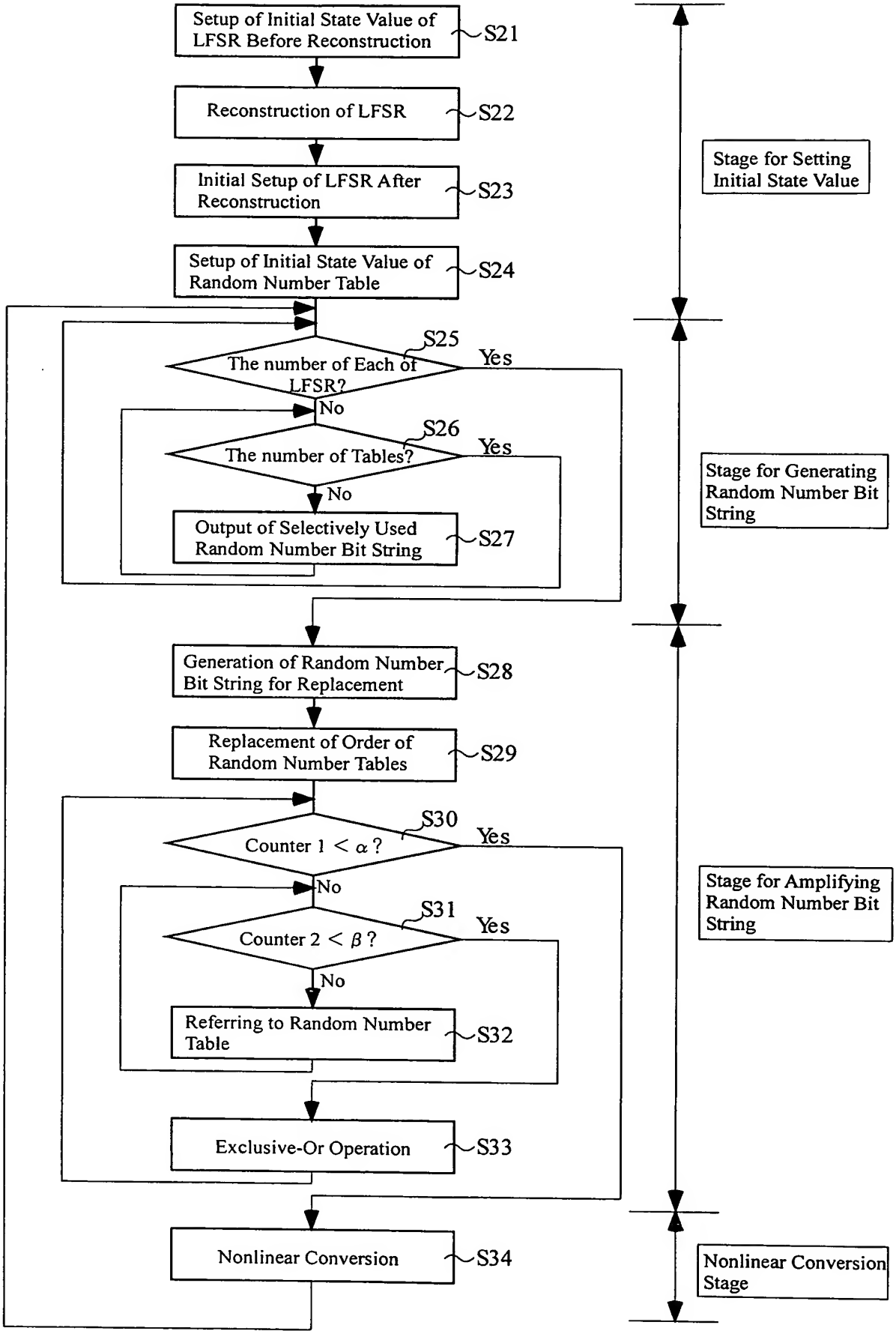

Setup of Initial State Value of LFSR Before Reconstruction
S21
Reconstruction of LFSR
S22
Initial Setup of LFSR After Reconstruction
S23
Setup of Initial State Value of Random Number Table
S24
Stage for Setting Initial State Value
S25
The number of Each of LFSR?
Yes
No
S26
The number of Tables?
Yes
No
Output of Selectively Used Random Number Bit String
S27
Stage for Generating Random Number Bit String
Generation of Random Number Bit String for Replacement
S28
Replacement of Order of Random Number Tables
S29
S30
Counter 1 < α ?
Yes
No
S31
Counter 2 < β ?
Yes
No
Referring to Random Number Table
S32
Exclusive-Or Operation
S33
Stage for Amplifying Random Number Bit String
Nonlinear Conversion
S34
Nonlinear Conversion Stage

FIG.11

LFSR1	I1(x)=x^129+x^80+x^8+x+1
LFSR2	I2(x)=x^131+x^80+x^16+x+1
LFSR3	I3(x)=x^133+x^16+x^8+x^2+1
LFSR4	I4(x)=x^137+x^20+x^12+x+1
LFSR5	I5(x)=x^139+x^80+x^12+x+1
LFSR6	I6(x)=x^143+x^56+x^12+x+1
LFSR7	I7(x)=x^149+x^84+x^8+x^2+1
LFSR8	I8(x)=x^151+x^60+x^8+x+1

FIG.12

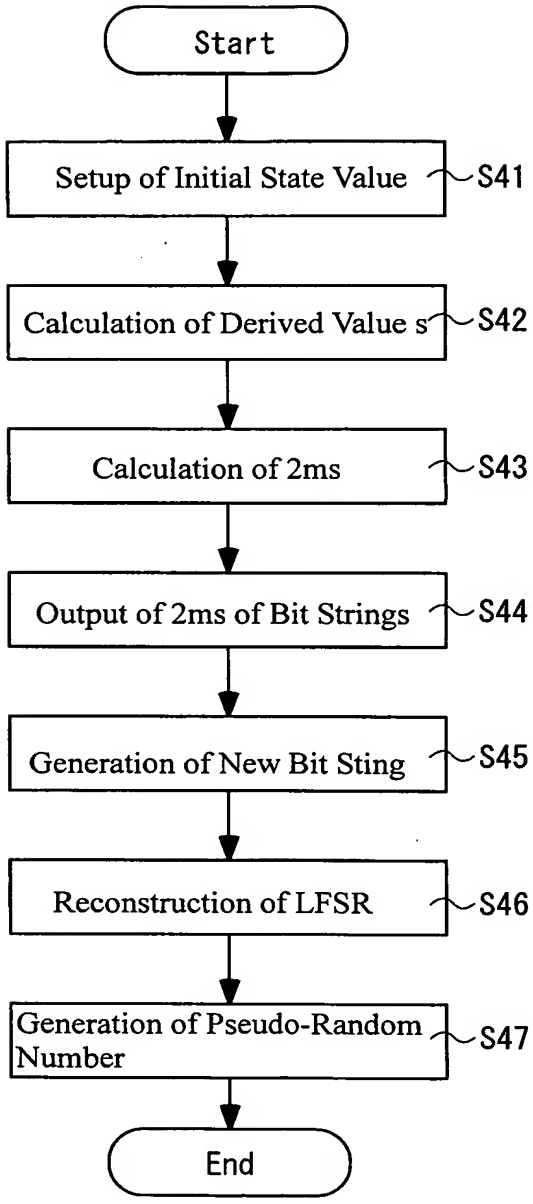

Start
Setup of Initial State Value
S41
Calculation of Derived Value s
S42
Calculation of 2ms
S43
Output of 2ms of Bit Strings
S44
Generation of New Bit Sting
S45
Reconstruction of LFSR
S46
Generation of Pseudo-Random Number
S47
End

FIG.13

Table 1: Throughput Measurement Result

Means Throughput of LFSR (151 Lines)	5.203Mbits/sec
Mean Throughput of RC4	141.6Mbits/sec
Mean Throughput of Replacement Processing	69.99Mbits/sec
Mean Throughput of Random Number Table	7.923Gbits/sec
Mean Throughput of Nonlinear Function	119.2Mbits/sec
Throughput of Whole Pseudo-Random Number Generator	116.4Mbits/sec
Mean Throughput of Conventional Type	0.680Mbits/sec

FIG.14

Table 2: Parameter of NIST

Data Length	1,000,000
Block Frequency Test Block Length	100
Non Overlapping Template Test Block Length	10
Overlapping Template Test Block Length	10
Universal Test Block Length	7
Universal Test Number Of Initialization Steps	1,280
Approximate Entropy Test Block Length	2
Serial Test Block Length	2
Linear Complexity Test Subsequence Length	500
bitstreams should be generated	10

FIG.15

Test Items	P-value
Frequency	0.987896
Block-Frequency	0.678686
Cusum	0.366918
Cusum	0.213309
Runs	0.383827
Long-Run	0.595549
Rank	0.798139
FFT	0.021999
Aperiodic-Template	0.867692
Aperiodic-Template	0.574903
Aperiodic-Template	0.779188
Aperiodic-Template	0.350485
Aperiodic-Template	0.798139
Aperiodic-Template	0.494392
Aperiodic-Template	0.867692
Aperiodic-Template	0.085587
Aperiodic-Template	0.474986
Aperiodic-Template	0.996335
Aperiodic-Template	0.249284
Aperiodic-Template	0.153763
Aperiodic-Template	0.514124
Aperiodic-Template	0.657933
Aperiodic-Template	0.595549
Aperiodic-Template	0.719747
Aperiodic-Template	0.996335
Aperiodic-Template	0.657933
Aperiodic-Template	0.759756
Aperiodic-Template	0.834308
Aperiodic-Template	0.851383
Aperiodic-Template	0.657933
Aperiodic-Template	0.494392
Aperiodic-Template	0.779188
Aperiodic-Template	0.883171
Aperiodic-Template	0.798139
Aperiodic-Template	0.719747
Aperiodic-Template	0.964295
Aperiodic-Template	0.401199
Aperiodic-Template	0.12962
Aperiodic-Template	0.739918
Aperiodic-Template	0.010555
Aperiodic-Template	0.202268
Aperiodic-Template	0.289667
Aperiodic-Template	0.897763
Aperiodic-Template	0.719747
Aperiodic-Template	0.494392
Aperiodic-Template	0.019188
Aperiodic-Template	0.066882
Aperiodic-Template	0.574903
Aperiodic-Template	0.699313
Aperiodic-Template	0.978072
Aperiodic-Template	0.153763
Aperiodic-Template	0.419021
Aperiodic-Template	0.851383
Aperiodic-Template	0.55442
Aperiodic-Template	0.897763
Aperiodic-Template	0.213309
Aperiodic-Template	0.319084

Test Items	P-value
Aperiodic-Template	0.657933
Aperiodic-Template	0.494392
Aperiodic-Template	0.987896
Aperiodic-Template	0.419021
Aperiodic-Template	0.350485
Aperiodic-Template	0.616305
Aperiodic-Template	0.935716
Aperiodic-Template	0.897763
Aperiodic-Template	0.897763
Aperiodic-Template	0.171867
Aperiodic-Template	0.739918
Aperiodic-Template	0.897763
Aperiodic-Template	0.224821
Aperiodic-Template	0.851383
Aperiodic-Template	0.419021
Aperiodic-Template	0.319084
Aperiodic-Template	0.401199
Aperiodic-Template	0.616305
Aperiodic-Template	0.911413
Aperiodic-Template	0.897763
Aperiodic-Template	0.897763
Aperiodic-Template	0.897763
Aperiodic-Template	0.080519
Aperiodic-Template	0.867692
Aperiodic-Template	0.115387
Aperiodic-Template	0.275709
Aperiodic-Template	0.779188
Aperiodic-Template	0.202268
Aperiodic-Template	0.319084
Aperiodic-Template	0.637119
Aperiodic-Template	0.739918
Aperiodic-Template	0.224821
Aperiodic-Template	0.514124
Aperiodic-Template	0.137282
Aperiodic-Template	0.964295
Aperiodic-Template	0.334538
Aperiodic-Template	0.678686
Aperiodic-Template	0.719747
Aperiodic-Template	0.080519
Aperiodic-Template	0.145326
Aperiodic-Template	0.319084
Aperiodic-Template	0.145326
Aperiodic-Template	0.304126
Aperiodic-Template	0.867692
Aperiodic-Template	0.719747
Aperiodic-Template	0.437274
Aperiodic-Template	0.030806
Aperiodic-Template	0.224821
Aperiodic-Template	0.514124
Aperiodic-Template	0.171867
Aperiodic-Template	0.010988
Aperiodic-Template	0.946308
Aperiodic-Template	0.162606
Aperiodic-Template	0.534146
Aperiodic-Template	0.574903
Aperiodic-Template	0.334538
Aperiodic-Template	0.699313

Test Items	P-value
Aperiodic-Template	0.616305
Aperiodic-Template	0.042808
Aperiodic-Template	0.759756
Aperiodic-Template	0.779188
Aperiodic-Template	0.262249
Aperiodic-Template	0.455937
Aperiodic-Template	0.55442
Aperiodic-Template	0.383827
Aperiodic-Template	0.12962
Aperiodic-Template	0.867692
Aperiodic-Template	0.759756
Aperiodic-Template	0.637119
Aperiodic-Template	0.867692
Aperiodic-Template	0.955835
Aperiodic-Template	0.897763
Aperiodic-Template	0.996335
Aperiodic-Template	0.115387
Aperiodic-Template	0.383827
Aperiodic-Template	0.275709
Aperiodic-Template	0.55442
Aperiodic-Template	0.051942
Aperiodic-Template	0.595549
Aperiodic-Template	0.657933
Aperiodic-Template	0.637119
Aperiodic-Template	0.045675
Aperiodic-Template	0.924076
Aperiodic-Template	0.978072
Aperiodic-Template	0.739918
Aperiodic-Template	0.455937
Aperiodic-Template	0.657933
Aperiodic-Template	0.574903
Aperiodic-Template	0.304126
Aperiodic-Template	0.249284
Aperiodic-Template	0.289667
Aperiodic-Template	0.946308
Aperiodic-Template	0.010535
Aperiodic-Template	0.816537
Aperiodic-Template	0.739918
Aperiodic-Template	0.350485
Aperiodic-Template	0.798139
Aperiodic-Template	0.455937
Aperiodic-Template	0.145326
Periodic-Template	0.657933
Universal	0.383827
Apen	0.534146
Random-Excursion	0.534146
Random-Excursion	0.213309
Random-Excursion	0.534146
Random-Excursion	0.035174
Random-Excursion	0.534146
Random-Excursion	0.534146
Random-Excursion	0.010879
Random-Excursion	0.213309
Random-Excursion-V	0.534146
Random-Excursion-V	0.739918
Random-Excursion-V	0.213309
Random-Excursion-V	0.911413

Test Items	P-value
Random-Excursion-V	0.035174
Random-Excursion-V	0.911413
Random-Excursion-V	0.350485
Random-Excursion-V	0.534146
Random-Excursion-V	0.350485
Random-Excursion-V	0.213309
Random-Excursion-V	0.213309
Random-Excursion-V	0.534146
Random-Excursion-V	0.534146
Random-Excursion-V	0.122325
Random-Excursion-V	0.213309
Random-Excursion-V	0.066882
Random-Excursion-V	0.035174
Serial	0.350485
Serial	0.289667
Lempel-Ziv	0.383827
Linear-Complexity	0.090936

FIG. 16

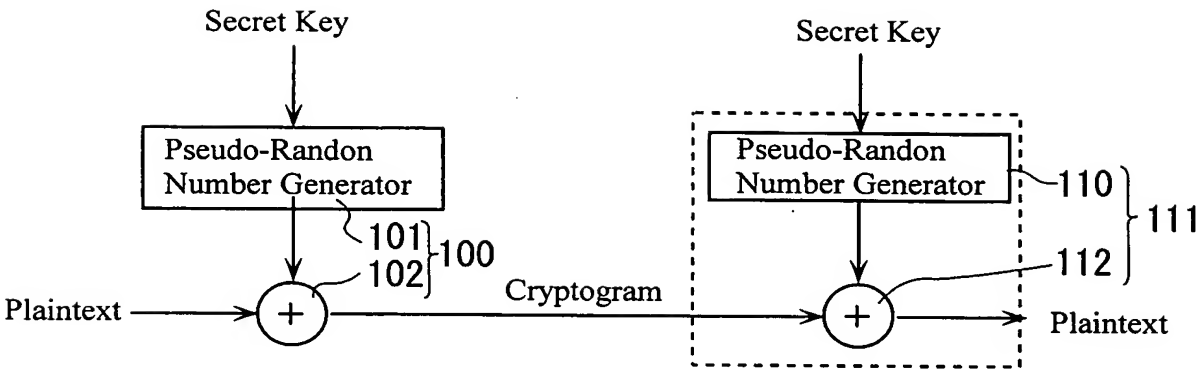

Secret Key
Pseudo-Randon Number Generator
101
102
100
Plaintext
Cryptogram
Secret Key
Pseudo-Randon Number Generator
110
111
112
Plaintext

FIG. 17

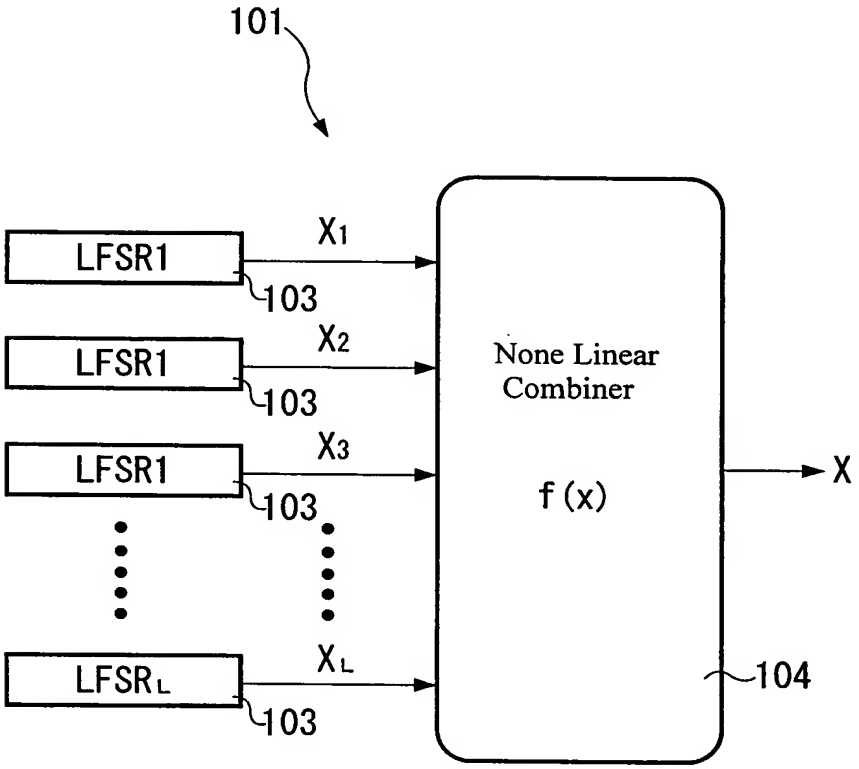
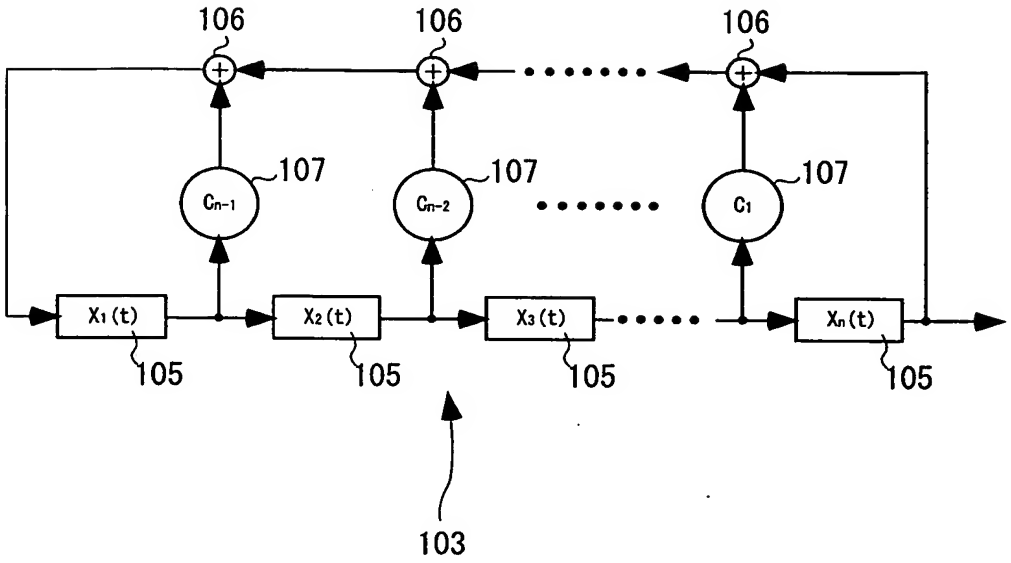

101
LFSR1
X1
103
LFSR1
X2
103
LFSR1
X3
103
LFSRL
XL
103
None Linear Combiner
f (x)
X
104

FIG. 18


106
106
106
107
107
107
Cn-1
Cn-2
C1
X1(t)
X2(t)
X3(t)
Xn(t)
105
105
105
105
103